

REMARKS/ARGUMENTS

Claims 1-9 and 15-16 are pending in this application.

This application was on appeal. The Patent Office has reopened prosecution and new rejections have been made.

The Examiner rejects claims 1-9 and 15-16 under 35 U.S.C. §112. In particular, the Examiner says that the recitation relating to the storing of subsets of the processed electronic pharmacy data in a data mart wherein the subsets are adapted to meet the specific demands of particular requestors in terms of analysis, content, presentation and ease of use thereby to allow preparation of predetermined sets of reports pertinent to the particular requestor, is vague and indefinite. In particular, the Examiner says it is unclear how the specific demands are met and it is unclear as to what is meant by "ease of use."

Referring to paragraphs 37 and 38 of the specification , the present invention stores the processed electronic pharmacy data in a data warehouse. Subsets of the processed electronic pharmacy data, i.e., a smaller portion than is stored in the data warehouse, are stored in the data mart. The subsets are adapted to meet specific demands of particular requestors in terms of analysis, content, presentation and ease of use. See paragraph 37 of the specification. In particular, these specific demands, i.e., in terms of analysis, content, presentation and ease of use for preparing reports for the particular users are met by storing only a portion of the larger set of data residing in the data warehouse. See paragraph 37. That is, the data mart is provided to store a subset or a smaller portion of the total electronic data that is stored in the data warehouse. This enables the preparation of reports pertinent to a particular requestor or group of requestors in terms of analysis, content, presentation and ease of use because only a smaller subset of the electronic information is stored in the data mart that is pertinent to those users. This provides for a faster and more efficient preparation of the reports.

Accordingly, the claim has been amended to specify how the specific demands are met, i.e., by storing a portion of a larger set of data residing in the data warehouse. Support for the amendment is provided in paragraph 37 in the specification. It is believed that this amendment addresses the Examiner's first concern as to how the specific demands are met.

With respect to the "ease of use" qualification, the specification in paragraph 37 identifies "ease of use" as a concern for the reports for specified requestors. "Ease of use" relates

to the ability to review the reports easily. Paragraph 38 elaborates on this. Paragraph 38 of the specification states that data is placed in a predetermined format to facilitate ease of review of the data by the requestor. The predetermined format may vary depending on the type of data received, but it is preferably a standard format for the data type to aid readability and minimize confusion. It is believed that the specification adequately addresses what is meant by “ease of use.” However, since the specification describes how the ease of use is obtained, i.e., by using specified formats, “ease of use” has been amended in the claim to “format”. Thus, the subsets of data are adapted to meet the specific demands of the particular requestors in terms of analysis, content, presentation and format. This allows preparation of predetermined sets of reports pertinent to the particular requestors.

It is submitted that the amendments adequately address the §112 issues and that in view of the amendments, the rejection under 35 U.S.C. §112 should be withdrawn.

Now turning to the rejection based on the prior art, the Examiner now rejects the claims under 35 U.S.C. §103 as being unpatenatable over Donoho in view of Schoenberg and Mehring. The new reference applied is Mehring.

In reviewing the Examiner’s new rejection, it appears that the Examiner is applying Mehring specifically to address the recitation of the subsets of data that are stored in the data mart. However, Applicants submit that the Examiner’s new rejection still fails to teach or suggest the invention. In particular, Applicants submit that the citation of the combined references still fails to teach or suggest the invention as claimed. As explained in detail below and in the Appeal Brief previously filed, Schoenberg, cited by the Examiner, fails to teach or suggest the first and second access security steps of the invention. The Examiner admits that Donoho does not teach these steps. However, the Examiner continues to insist that Schoenberg teaches the steps of providing the first and second access security. However, as explained in the previously filed Appeal Brief, and as explained herein, Schoenberg and Donoho taken together fail to teach or suggest the steps of providing the first and second access security. Mehring, now cited, does not add anything to the combined teachings of Donoho and Schoenberg which would teach or suggest the first and second access security steps. In particular, Applicants address the new combination of references, that is, Donoho, Schoenberg and Mehring as follows.

The Examiner's primary reference is Donoho. Donoho describes a method and apparatus whereby a collection of computers and associated communications infrastructure operate according to a communications process. This process allows information providers to broadcast information to a population of information consumers. The information may be targeted to those consumers who have a precisely formulated need for the information. This targeting may be based on information that is inaccessible to other communication protocols. For example, under other protocols, the targeting requires each potential recipient to reveal sensitive information because under other protocols, the targeting requires each potential recipient to reveal information obtainable only after extensive calculations using data available only upon intimate knowledge of the consumer computer, its contents and local environment.

According to the Examiner, Donoho teaches a method for storing and reporting pharmacy data comprising the steps of generating by a plurality of pharmacies (see Donoho, column 53, lines 4-6 and column 92, lines 25-39), each of the pharmacies operating within a managed care organization, electronic pharmacy data comprising medical, financial and transactional information related to pharmaceutical transactions. The Examiner points to column 53, lines 4-6 and column 92, lines 25-39.

The Examiner asserts that Donoho teaches providing a report to a requestor. The Examiner refers to column 53, lines 5-6 and column 53, lines 17-20. The Examiner asserts that Donoho teaches receiving over a network by a processing center of a managed care organization a data transfer request to transfer respective electronic pharmacy data from at least one of the plurality of pharmacies.

The Examiner concedes that Donoho does not teach the remaining elements of Applicant's claim 1, in particular starting with providing the first and second access securities. However, the Examiner asserts that Schoenberg teaches all remaining steps of Applicant's claim 1 including providing the first and second access security, the step of receiving the transfer of the respective electronic pharmacy data, organizing and structuring the electronic pharmacy data and storing the processed electronic pharmacy data in a data warehouse including subsets of the electronic pharmacy data.

The Examiner further asserts that Schoenberg teaches receiving a data request from a data requestor and providing the third and fourth access security, formatting the portion

of the electronic pharmacy data requested by the data requestor and providing the report to the requestor.

The Examiner's contentions are without merit. The present invention relates to a method for storing and reporting pharmacy data. The pharmacy data is generated by a pharmacy and is received at the processing center after first and second access security checks. The first access security check determines that the pharmacy submitting the data has the proper credentials. The second access security check determines that the data itself meets at least one predefined validity requirement defined by the processing center. Thus, according to the invention, both the credentials of the sending pharmacy and the validity of the data sent are checked before the data is stored and processed.

Assuming that the data meets the first and second access security, it is processed, organized, structured and stored in the data warehouse.

The second aspect of the Applicant's invention is that once a data request is received to request data from the data warehouse, there are third and fourth access securities. The third access security checks the credentials of the requestor, i.e., whether the requestor is authorized. The fourth access security checks the privilege level of the data requestor so that only data consistent with the requestor's privilege level is allowed to be submitted to the requestor.

Thereafter a report is provided based upon the requestor's privilege level.

The Examiner relies on the Schoenberg reference for the teachings of the first, second, third and fourth access security. However, the Examiner is mistaken about Schoenberg. Schoenberg discloses a system for distributing health information. The Examiner asserts that Schoenberg teaches the first and second access security. However, the Examiner is incorrect. Schoenberg does describe certain forms of access security, but they are not the access security as claimed. In column 6, lines 26-50 with reference to Figs. 2 and 3, Schoenberg receives health information and generates security access codes 202, (see Fig. 2) and assigns one or more security access codes to each of the categories of health information. However, Schoenberg does not teach or suggest what Applicant's invention does. Applicant's invention will receive and process the information from the pharmacies if it passes the first and second access security. In contrast, in the Schoenberg reference, there is no provision for determining whether the

information that is received is reliable and whether it should be received and processed in the first place, i.e., there is nothing in Schoenberg which teaches or suggests passing first and second access securities before the information is received and processed. Schoenberg receives the information and then categorizes it and assigns access codes to it so that if a request is later made for that information, the request will only be granted if the access codes are met.

Schoenberg requires access codes to retrieve the information from the system as requested by a data requestor. Schoenberg does not teach or suggest verifying the information in the first place before it is stored in the system for later retrieval. Thus, Schoenberg fails to teach or suggest providing first access security by the processing center in response to the data transfer request, wherein the first access security includes checking credentials defined by the processing center and submitted for authorization by the at least one pharmacy. The Examiner has confused the "data transfer in" portion for the "data transfer out" portion, i.e., Schoenberg does not teach or suggest providing first access security for receiving information ("transfer in") Schoenberg merely teaches assigning security codes and then when a request for data transfer ("transfer out") is made, checking to see that the user provides the previously provided access code. Thus, at most, Schoenberg may suggest the third access security step of the claims, that is, checking credentials submitted for authorization by the data requestor. However, Schoenberg suggests nothing about providing first access security in order to determine whether the provider of the information is entitled to provide the information in the first place. Furthermore, Schoenberg does not teach or suggest the second access security step which relates to checking the validity of the data itself presented by the data provider. According to the present invention, prior to accepting the respective pharmacy data by the processing center, the data is checked to determine whether it meets at least one predefined validity requirement defined by the processing center. Schoenberg utterly fails to teach or suggest the second access security step.

The Examiner makes much of the fact that Schoenberg teaches a tiered security access as shown in Figs. 2-3 and discussed in column 3, lines 20-52, i.e., that the provider of the information can provide high levels of security for data that it wishes to secure at a higher level. The Examiner is again confusing the security access when data is retrieved from the system with the security access also provided by the present invention for providing data to the system. According to the present invention, the provider of the data is checked to determine if it meets a

first access security and the data itself is checked to determine whether it meets a second access security, i.e., that it is valid data. There is nothing in Schoenberg that teaches the first and second access security.

The Examiner has asserted that Donoho teaches the step of checking that the data meets at least one predefined validity requirement, i.e., the second access security step. The Examiner points to Donoho, column 21, lines 9-16 in particular, for verification of the integrity of the message by computing a functional from the message. The Examiner asserts that this supports the teaching of the first access security step. Further, the Examiner cites Schoenberg, column 6, lines 26-52 and the table at columns 5-6 as teaching the checking of credentials submitted for authorization by the at least one pharmacy.

The checking of credentials such as user names and passwords described in column 6, lines 26-52 and the table in columns 5-6 of Schoenberg relates to the request for data from the system. Thus, according to Schoenberg, the access security codes generated originally by the patient are checked to determine that the requestor of the information is authorized to receive the information. This does not suggest that a first access security step be implemented when the data is received, i.e., whether the data received from the pharmacy should be processed and stored in the first place. Schoenberg relates to the transfer of data out of the system but does not relate to whether the data should be stored in the system in the first place.

The Examiner asserts that Donoho at column 21, lines 9-16, through its description of a digital digest that can be appended to the message for ensuring message integrity, suggests Applicant's claimed second access security. However, taken as a whole, Donoho and Schoenberg do not teach or suggest Applicant's claim 1 which provides for receiving data, checking a first access security and a second access security before storing and processing the data and furthermore, providing a third access security and a fourth access security when a request for the data that is stored is received. Applicant submits that the combination of Donoho and Schoenberg fails to teach or suggest all the steps of Applicant's claim 1. Accordingly, Donoho and Schoenberg, taken together, do not render independent claim 1 obvious.

The Mehring reference has now been cited by the Examiner for the proposition that it teaches a method step of sorting data into restricted and unrestricted data where the data is sorted into multiple levels of restricted data with each requiring another security level to access.

The Examiner concludes that one of ordinary skill in the art at the time of the invention would have found it obvious to combine the method of storing and reporting pharmacy data as taught by Donoho with the secure data access taught by Schoenberg with the multiple levels of restricted data as taught by Mehring with the motivation to distribute medical information in which the medical care provider or pharmacy has quick access to a patient's medical record, but only to the information within the medical record that is needed by the user (medical professional, doctor, nurse) for the proper treatment of the patient at the time.

The Examiner's stated conclusion, however, misses the entire point that Applicants have been making all along through the prosecution of this application, including on the Appeal. The combination of references, and in particular, the Schoenberg reference, fails to teach or suggest the steps of providing the first and second access securities. These steps, relate not to a request for data by a data requestor, which is the province of the third and fourth access securities according to the invention, but instead relate to a data transfer request to transfer data from the pharmacy into the data warehouse. Schoenberg does not teach or suggest providing access securities when a data transfer request into the system is being made. According to the present invention, the first and access securities are provide to verify that the transferor is entitled to make the transfer of data into the system, not to request data out of the system. Schoenberg only relates to providing access securities which are chosen by the patient, see column 6, lines 29-30, to ensure that the patient can obtain access to the data that has been previously stored. There is nothing in Schoenberg which relates to ensuring in the first place that the data that is being stored is being transferred by an entity that has the proper credentials to store the data in the first place and that the data itself that is being stored is valid. This is what the first and second access security steps relate to and there is nothing in Schoenberg or in Donoho or Mehring that relates to this,. In particular, these steps which are not taught or suggested by the combination of references, recite as follows:

“receiving, over a network by a processing center of the managed care organization, a data transfer request to transfer respective electronic pharmacy data from at least one of the plurality of pharmacies;

providing first access security by the processing center in response to the data transfer request, wherein the first access security includes checking credentials defined by the

processing center and submitted for authorization by the at least one pharmacy; and

providing second access security by the processing center in case the at least one pharmacy passes the first access security, wherein the second access security includes, prior to accepting the respective electronic pharmacy data by the processing center, checking whether the respective electronic pharmacy data meet at least one predetermined validity requirement defined by the processing center.”

It is only after the request is made to transfer data and the first and second access security steps are implemented, and passed by the transferor, that the step of “receiving by the processing center, a transfer of the respective electronic pharmacy data pursuant to compliance with the second access security” is achieved.

None of these steps is taught or suggested by Schoenberg, taken in combination with Donoho and the Mehring references. In short, the combination of references cited by the Examiner wholly fails to teach or suggest the data transfer in request and the first and second access security steps which enable the data to be received by the processing center. There is no teaching or suggestion accordingly, of the subject matter of the claims in the combination of Donoho, Schoenberg and Mehring.

Accordingly, for the above reasons, it is submitted that the rejection of the claims under 35 U.S.C. §103, based upon Donoho, Schoenberg and Mehring, should be withdrawn and in view of the amendments to address the §112 rejection, this application should be passed to issue.

Respectfully submitted,



Louis C. Dujmich
Registration No.: 30,625
OSTROLENK FABER LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

LCD/jh